UNITED STATES DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION

STATEMENT OF ROBERT JAMISON
DEPUTY ADMINISTRATOR

Before the

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTE ON FEDERAL WORKFORCE AND AGENCY ORGANIZATION

April 4, 2006

Good afternoon, Chairman Porter, Ranking Member Davis, and Members of the Subcommittee. Thank you for this opportunity to discuss the Transportation Security Administration's (TSA) role in enhancing aviation security and how we work with Federal, State, and local partners in the management and operation of our Nation's airports. It is a pleasure to appear before the Subcommittee with the distinguished representative of the Office of Personnel Management -- an agency with whom we coordinate in carrying out our aviation security mission.

The Role of the Transportation Security Administration

Created in the aftermath of the 9/11 terrorist attacks with the Aviation and Transportation Security Act (ATSA), P.L. 107-71, as its statutory foundation, TSA has worked with the airlines, airports, the shipping industry, flight crews, law enforcement, and passengers to take aviation security orders of magnitude beyond where it stood on 9/11. Today we have numerous independent layers of security that, together, create a formidable security network. These layers include checking passenger manifests against terrorist watch lists; physical screening of passengers; physical screening of carry-on bags and checked baggage; airport security regulations and inspections; and the presence of Federal Air Marshals and TSA-authorized armed Federal Flight Deck Officers on flights. These measures also include systems for vetting and physically screening TSA employees, airline employees, and airport workers who have access to secure areas of our airports. Based on the particular interests of the Committee, my testimony today will focus on the vetting and screening systems for TSA employees and others who have access to secure airport areas.

Vetting Federal Employees, Contractors, Airline and Airport Personnel

All TSA, airline, airport, and airport vendor employees or contractors who have access to secure areas in regulated airports have undergone extensive background checks.

TSA Transportation Security Officers, who conduct passenger, baggage, and cargo screening at airports, undergo a two-part background investigation process. TSO applicants are first subject to a pre-employment background investigation. This investigation features the Office of Personnel Management (OPM) Special Agreement Check which is a fingerprint based criminal history check that is processed through the FBI. If the pre-employment investigation is favorable and the applicant accepts a position with TSA, the individual then is subject to further background checks through OPM's Access National Agency Check with Inquiries (ANACI). The TSO is permitted to begin employment while the ANACI is underway. If derogatory information is developed, the individual is afforded an opportunity to address the information obtained during the investigation. If the information is not favorably resolved, the individual is removed from Federal service.

Other TSA employees undergo a similar investigation process. A pre-employment check is conducted to determine suitability, followed by a second, more in-depth investigation. The particulars of the second investigation are determined by the level of access required for the position (e.g., Secret or Top Secret) after the employee begins employment. According to OPM's quarterly report for the first quarter of fiscal year 2006 (October 1, 2005 to December 31, 2005) a Minimum Background Investigation for TSA employees who require access to Secret information takes approximately 27 days when priority service is required, and 106 days when standard service is needed.

All airline and airport employees and contractors who require unescorted access to secure areas of the airport are subject to both fingerprint-based criminal history record checks and name-based background checks. Prior to employment, airlines and airports send fingerprints and other biographical information to the American Association of Airport Executives (AAAE) Transportation Security Clearinghouse, which conducts quality control on the information, accepts paper and electronic fingerprint submissions, converts the paper fingerprint submissions into an electronic format, and formats all data received into a single format for TSA. TSA then transmits to the FBI the necessary biographical information and fingerprint data to conduct a criminal history records check. The FBI returns the results of its criminal history records check to TSA's secure Fingerprint Results Distribution website, where airline and airport employer security representatives can access the information and adjudicate the results based on 28 disqualifying criminal offenses, which include forgery, unlawful possession of a weapon or explosive material, interfering with a flight crew or flight attendants, certain violent crimes causing bodily injury or death, treason, extortion, arson, and conspiracy. The disqualifying offenses are identified in section 44936(b) of Title 49 United States Code and implemented by 49 CFR 1542.209(d).

Simultaneous with the FBI's criminal history records check, TSA conducts a name-based security threat assessment against approximately ten databases that include information related to suspected or actual terrorist activity, suspicious immigration and identify theft activity, and criminal wants and warrants. Beginning in September 2005, TSA began using a system of "perpetual" name-based vetting of all TSA, airline, airport,

and airport vendor employees and contractors. Under this system, each time a name is added to any one of the databases, all individuals who currently have unescorted access to secure areas are immediately checked against the new information.

Any applicant that meets the minimum criteria established by TSA as a possible match with information contained in these databases (during the course of the initial check or as part of the perpetual vetting process) undergoes further analysis. If, after that additional review, an individual is determined to pose or is suspected of posing a security threat, information about that individual is sent to appropriate law enforcement or intelligence agencies for further analysis. The law enforcement or intelligence agencies determine whether the individual's identity can be verified and whether he or she continues to pose a threat or is suspected of posing a threat, and notifies TSA. TSA informs airlines or airports when an individual's access to secure areas must be denied or rescinded. Individuals are given an opportunity to correct any incorrect underlying identification or court records. Based on the information provided through this process, law enforcement or intelligence agencies may take further action with respect to an individual for whom derogatory information is found.

Approximately 1,100 applicants are vetted each week. As of January 31, 2006, there were 695,564 active Security Identification Display Area (SIDA) badges and 85,013 active sterile area badges nationwide. Sterile areas are those areas beyond the passenger screening checkpoint, but inside the terminal area. SIDA badges are required to access areas beyond alarmed doors that are used for airport operations, where individuals can access the flight line, ramp, or aircraft.

Access Control to Sterile and Security Identification Display Areas

Generally, in order to access sterile areas of the airport, individuals who do not possess SIDA badges, including airport and airline personnel, vendors and contractors, and even TSA employees, must pass through the TSA security screening checkpoint. At these checkpoints, highly trained and motivated TSA Transportation Security Officers (TSOs) use complex specialized equipment, hand searches of carry-on bags, and pat-downs of individuals to identify and find weapons and explosive devices. This is the same physical screening process that passengers must pass through before boarding an aircraft. TSOs who work at security screening checkpoints receive extensive training, including an initial 49.5 hours of classroom training and 65 hours of on-the-job training, and approximately 3 hours of refresher training on a weekly basis. Additional classroom and on-the-job training is required to conduct baggage screening.

Access to SIDA areas must be controlled and limited to authorized personnel, such as flight crews, cleaning crews, construction crews, and ramp crews. Control systems may include alarmed doors or gates, which are locked or guarded. When in a SIDA, an approved individual must display at all times a SIDA identification badge on their person above the waist and visible on their outermost garment. If individuals who are not cleared for unescorted access to the SIDA area require access to that area, they must be

accompanied or monitored by someone who has unescorted access and escort authority for that area. In addition, each airport operator must also establish and carry out a challenge program that requires every individual with unescorted access authorization to secured areas, including SIDA areas, to ascertain or challenge the authority of an individual who is not displaying proper badge identification while present in the area, and to take action in accordance with the airport security program.

Accountability

Airport operators are responsible for developing and implementing TSA-approved airport security programs which set forth procedures and processes to secure sterile areas and SIDA, as well as other important security procedures. TSA works closely with airport managers in developing and approving these programs, recognizing that the unique features of each airport may require special provisions.

Among other responsibilities, airport operators are required to:

- Create and issue identification badges that –
  - convey a full face image with full name, employer, and identification number,
  - clearly indicate the scope of an individual's access privileges,
  - clearly indicate an expiration date, and
  - are of sufficient size and appearance to be readily observable;

.

- Retrieve expired identification badges of individuals who no longer have unescorted access authority;

- Promptly report lost or stolen identification badges;

- Secure unissued identification badges and supplies;

- Audit the system as necessary, but at least once a year;

- Revalidate the identification system if a minimum threshold of unaccounted badges is reached;

- Reissue identification badges if badges are lost, stolen, or otherwise unaccounted for; and

- Ensure that only one identification badge is issued per individual at a time, unless because of his or her work, the individual is required to have more than one identification badge.

Compliance with the airport security program and Federal security regulations is verified by almost 1,000 TSA Aviation Security Inspectors (ASIs) including approximately 300 air cargo security inspectors. They conduct regular and unpredictable inspections,

identify security vulnerabilities and make recommendations to overcome those vulnerabilities, and investigate alleged violations of security regulations.

Closing

Mr. Chairman, TSA's mission is to protect the Nation's transportation systems while facilitating the movement of people and commerce. As part of our risk-based strategic approach to aviation security, we work closely with our government and industry partners to ensure that workers with access to the most secure areas of our Nation's airports have been thoroughly vetted and that access to those areas is limited to authorized individuals.

Thank you again for the opportunity to testify today. I would be happy to respond to questions.